FIABILITÉ DES CAPTEURS-TRANSMETTEURS INTÉGRANT DES FONCTIONNALITÉS NUMÉRIQUES

RELIABILITY OF TRANSMITTERS BASED ON DIGITAL FUNCTIONALITIES

Florent Brissaud & Dominique Charpentier
Institut National de l'Environnement Industriel et des Risques
Parc Technologique ALATA, BP 2
60260 Verneuil-en-Halatte, France
Tel. : +33 3 44 55 69 89 (F. Brissaud)
Courriel : florent.brissaud@ineris.fr

Anne Barros & Christophe Bérenguer
Université de Technologie de Troyes
Institut Charles Delaunay
STMR UMR CNRS 6279
12 rue Marie Curie, BP 2060
10010 Troyes cedex, France

Résumé

Les travaux présentés s'inscrivent dans le cadre d'une thèse réalisée à l'INERIS et sous la direction scientifique de l'UTT. Ils portent sur l'évaluation de la fiabilité des capteurs-transmetteurs intégrant des fonctionnalités numériques. Ces systèmes sont communément qualifiés « d'intelligents » car capables d'effectuer des fonctionnalités innovantes de types autodiagnostics, autocorrections d'erreurs, et reconfigurations. De plus, ils peuvent exploiter une communication numérique bidirectionnelle afin de réaliser des opérations en « collaboration ». L'évaluation de ces capteurs a tout d'abord considéré ces derniers de façon « autonome » en développant une modélisation qui tienne compte des interactions internes (matérielles et fonctionnelles), à partir de laquelle des analyses de fiabilité ont été proposées. De plus, les incertitudes liées aux comportements dysfonctionnels et souvent mal connus de ces systèmes ont été traitées. Ensuite, une approche plus « systémique » a été développée, intégrant ces capteurs dans un système de contrôle relatif à la sécurité, et prenant en compte les interactions entre tous les éléments du système, ainsi qu'avec le processus contrôlé, traitant alors avec des problèmes de fiabilité dynamique.

Summary

These works are part of a PhD thesis performed at the INERIS, under the scientific supervision of the UTT, and about the reliability of digital-based transmitters. These systems are commonly described as "intelligent" since they are able to perform innovative functionalities such as self-diagnoses, error measurement corrections, self-adjustments, and on-line reconfigurations. Moreover, they may take advantage of a bidirectional digital communication to perform "cooperating" operations. First, an "intelligent transmitter" modelling has been developed, which includes material and functional interactions, and reliability analyses have been proposed based on this model, dealing with uncertainties linked to system behaviours under faulty conditions. Then, "intelligent transmitters" taking part of control systems have been considered, taking the system elements interactions into account, as well as the process influences, using a dynamic reliability framework.

1. Contexte Industriel

1.1. La Maîtrise des risques technologiques et le contexte réglementaire français

Depuis les Révolutions Industrielles des XVIIIème et XIXème siècles, le développement de nouvelles technologies n'a cessé de croître, et souvent à des allures exponentielles (cf. Lois de Moore). Aujourd'hui, le contexte est celui de la globalisation. Les systèmes doivent alors répondre à de constantes évolutions et à des performances accrues, tout en faisant face à de très fortes contraintes économiques, humaines, et à des ressources limitées. Cela a conduit au développement de technologies de plus en plus critiques pour la sécurité. Les exemples se trouvent dans de nombreux secteurs d'activités : l'énergie (les puissances des centrales, le nucléaire, les exploitations offshores), le transport (la capacité des avions, la vitesse des trains), l'industrie en général (l'utilisation de nouveaux produits, de nouvelles technologies). La maîtrise des risques liés aux activités technologiques est alors devenue une nécessité sociétale, environnementale, et économique. Pour répondre aux exigences de l'ensemble de ces domaines, l'évaluation des risques doit faire face à plusieurs défis, dont celui de prendre en compte de la manière la plus efficace et la plus réaliste toute la complexité grandissante des systèmes.

Un risque est caractérisé par un scenario (ou un évènement), une probabilité (ou parfois une fréquence), et une gravité (conséquences non désirées). L'approche naturelle et la plus complète d'une évaluation d'un risque est donc une approche probabiliste. En France, les évaluations probabilistes des risques ne sont pas nouvelles en ce qui concerne les centrales nucléaires. En revanche, pour l'industrie en général, la réglementation sur la maîtrise des risques technologiques n'a intégré des critères probabilistes qu'après la catastrophe d'AZF à Toulouse, en septembre 2001. Ce sont les plans de prévention des risques technologiques (PPRT), créés par la « loi Risques » du 30 juillet 2003, puis précisée par le décret du 7 septembre 2005, qui introduisent pour la première fois la notion « d'aléa technologique », modifiant ainsi un cadre réglementaire « déterministe » établi au milieu des années 1970 [1]. Les PPRT reposent principalement sur la réglementation des installations classées pour la protection de l'environnement (ICPE), qui est régie par le Code de l'Environnement (cf. Livre V). Les ICPE comprennent les régimes de déclaration (D), d'enregistrement (E), et d'autorisation avec ou sans servitudes d'utilité publique (A ou AS). Les PPRT concernent les établissements AS, (plus de 600 en France), dits aussi « SEVESO seuil haut » selon les directives européennes, et visent à maîtriser l'urbanisation aux abords de ces installations. Avec la « loi Risques », la réglementation sur les études de danger (EDD) a également évolué afin d'intégrer des critères probabilistes, en particulier via l'arrêté du 29 septembre 2005. Ainsi, toutes les ICPE soumises à autorisation (A ou AS), (environ 50.000 en France), doivent fournir une EDD qui a pour but de caractériser, analyser, évaluer, prévenir et réduire les risques de l'installation, ainsi que de préciser l'ensemble des mesures de maîtrise des risques mises en œuvre. L'EDD donne lieu à « une analyse de risques qui prend en compte la probabilité d'occurrence, la cinétique et la gravité des accidents potentiels selon une méthodologie qu'elle explicite » et « elle définit et justifie les mesures propres à réduire la probabilité et les effets de ces accidents » (cf. Code de l'Environnement, Article L512-1).

1.2. Le Rôle de l'INERIS dans la maîtrise des risques technologiques

L'Institut National de l'Environnement Industriel et des Risques (INERIS) est un établissement public à caractère industriel et commercial (EPIC), placé sous la tutelle du Ministère de l'Écologie, de l'Énergie, du Développement Durable et de la Mer (MEEDDM), (appellation en vigueur début 2010). La mission principale de l'INERIS est de réaliser des études et des recherches permettant de prévenir les risques que les activités économiques font peser sur la santé, la sécurité des personnes, les biens, et l'environnement, et de fournir toute prestation destinée à faciliter l'adaptation des entreprises à cet objectif. L'INERIS effectue ainsi à la fois une mission de service public, pour l'État et les collectivités (programmes de recherche, appuis techniques, formations), et des prestations commerciales, d'étude et de conseil, pour des clients privés.

En ce qui concerne la maîtrise des risques technologiques, l'INERIS intervient à deux niveaux : celui des installations industrielles, notamment par la mise en œuvre de PPRT et la réalisation d'EDD ; et celui des équipements, en particulier par l'évaluation de dispositifs de sécurité. Sur ce dernier point, l'INERIS est doté d'une direction de la certification qui est notamment accréditée pour certifier des systèmes selon les normes en sécurité fonctionnelle CEI 61508 et CEI 61511. Afin de répondre à ses missions, l'INERIS exprime donc des besoins de recherche pour développer des outils méthodologiques et des référentiels pour l'évaluation probabiliste des risques industriels et de la sûreté de fonctionnement des systèmes.

1.3. Des Défis liés à l'innovation pour la maîtrise des risques : l'exemple des « capteurs-transmetteurs intelligents »

Le développement de nouvelles technologies nécessite une évolution conjointe des outils méthodologiques d'évaluation des risques et de sûreté de fonctionnement. L'exemple que nous développons dans la suite de ce papier concerne les « capteurs-transmetteurs intelligents ». À l'origine, un capteur est destiné à collecter des données issues de grandeurs physiques ou chimiques, exploitables par des systèmes tiers. Depuis les années 1980, l'émergence des microsystèmes électromécaniques a ensuite permis à ces capteurs d'intégrer de façon autonome le traitement de ces données, et ainsi de transmettre des signaux élaborés. Ces capteurs devenus « capteurs-transmetteurs » tirent également profit des technologies numériques pour effectuer des fonctionnalités innovantes, ce qui leur confère communément le qualificatif « d'intelligent » : la correction des erreurs de mesure, l'auto-ajustage, l'autodiagnostic et la validation des informations transmises, la reconfiguration en ligne (métrologique ou fonctionnelle), et la communication numérique et bidirectionnelle [2]. Les utilisateurs de ces systèmes bénéficient alors de meilleurs résultats de mesures, de réductions de coûts, et de facilité d'utilisation, ce qui conduit à une utilisation de plus en plus répandue des « capteurs-transmetteurs intelligents » dans tous les secteurs industriels, y compris pour des applications liées à la sécurité. De nouvelles problématiques apparaissent alors pour la maîtrise des risques, que nous pouvons par exemple présenter selon des critères de performance relatifs à la sûreté de fonctionnement : la fiabilité, la maintenabilité, et la sécurité.

Du point de vue de la fiabilité, certains défauts ou défaillances peuvent être en partie compensés par des procédures de tolérance aux anomalies (reconfiguration). De plus, les auto-ajustages peuvent prévenir l'apparition de dérives ou d'autres défauts et défaillances qui apparaissent avec le temps, et la communication numérique est souvent jugée plus fiable que l'analogique. En revanche, la plus grande quantité d'électronique, d'unités programmées, et de logiciels, implique de nouvelles causes et modes de défaillance qui sont souvent mal connus et difficiles à appréhender. De plus, chaque défaut ou défaillance peut influencer plusieurs fonctions du système et données transmises (résultats de mesure, informations de diagnostics). Enfin, la communication numérique fait encore l'objet de plusieurs interrogations, notamment face aux causes communes de défaillance. Du point de vue de la maintenabilité, des informations sur les dérives, les facteurs d'influence, les charges de sollicitation, les précédents défauts et défaillances observés avec les circonstances correspondantes, peuvent être surveillés au cours du temps et utilisés pour de la maintenance préventive. De plus, la communication numérique et les reconfigurations en ligne peuvent rendre des maintenances correctives simplifiées et plus efficaces. En revanche, une expertise particulière est nécessaire pour maintenir pleinement de tels systèmes devenus plus complexes. Enfin, du point de vue de la sécurité, les autodiagnostics permettent une meilleure détection des défauts et défaillances, et des états « sûrs » peuvent être définis avec plus de détails. La centralisation des données et la communication numérique peuvent également contribuer à une meilleure efficacité du management des risques. En revanche, les capteurs-transmetteurs deviennent de plus en plus des « boîtes noires » qu'ils convient donc de modéliser et d'analyser avec des outils appropriés.

1.4. Une Thèse de doctorat sur la fiabilité des capteurs-transmetteurs intégrant des fonctionnalités numériques

Afin de contribuer à l'effort de recherche et répondre aux défis présentés dans la Section 1.3, une thèse de doctorat a été initiée en 2007 à l'INERIS sur la « modélisation et l'évaluation de la fiabilité des systèmes relatifs à la sécurité intégrant de nouvelles technologies », avec des applications particulières aux « capteurs-transmetteurs à fonctionnalités numériques ». L'encadrement scientifique de cette thèse est assuré par l'Université de Technologie de Troyes (UTT), qui accueille l'Institut Charles Delaunay (ICD) dont le cadre thématique se définit autour des « Sciences et Technologies pour la Maîtrise des Risques ».

La thèse de doctorat s'est alors organisée autour de trois axes : 1) l'évaluation des performances des systèmes relatifs à la sécurité en général, notamment en se référant aux critères définis par la norme CEI 61508 ; 2) l'introduction aux problématiques liées à l'utilisation de nouvelles technologies pour des systèmes relatifs à la sécurité, et l'évaluation de la fiabilité des « capteurs-transmetteurs intelligents » ; 3) la considération des « capteurs-transmetteurs intelligents » en tant qu'éléments de systèmes de contrôle-commande avec des applications liées à la sécurité, et l'évaluation de la fiabilité de ces systèmes. Le premier axe a donné lieu au développement d'expressions analytiques pour l'évaluation des probabilités de défaillance de systèmes relatifs à la sécurité, généralisées aux architectures redondantes et avec la prise en compte de tests de révisions complets et partiels [3] ; ainsi qu'une méthodologie pour évaluer les taux de défaillance (données d'entrée des expressions précédentes) en fonction des facteurs d'influence propres à chaque système [4]. Le second axe a permis une investigation des notions et des problématiques liées aux « capteurs-transmetteurs intelligents » ; de développer une modélisation de ces systèmes qui permette de répondre aux problématiques identifiées ; et de formaliser l'évaluation de la fiabilité de ces systèmes, sur les bases du modèle proposé. Une partie de ces travaux a été présentée lors du 16ème congrès de maîtrise des risques et de sûreté de fonctionnement (Lambda-Mu 16, à Avignon, en 2008) [2]. La Section 2 de ce papier s'inscrit dans la continuité de ces travaux en proposant une extension du modèle initial, ainsi que les analyses associées. Enfin, le troisième axe de la thèse est consacré à une approche plus globale (ou « systémique »), prenant en compte les interactions entre plusieurs « capteurs-transmetteurs intelligents » d'un même système de contrôle-commande, entre des « capteurs transmetteurs intelligents » et d'autres éléments de ce système, ainsi qu'avec le processus contrôlé, traitant alors avec des problèmes de fiabilité dynamique. Une partie de ces résultats est présentée dans la Section 3 de ce papier.

2. Fiabilité des « Capteurs-Transmetteurs intelligents » en tant que Systèmes

2.1. Problématiques pour l'évaluation de la fiabilité des « capteurs-transmetteurs intelligents »

De précédents travaux de recherche ont été consacrés à la sûreté de fonctionnement de « systèmes distribués » (cf. Section 3.1) dont font généralement partis les « capteurs-transmetteurs intelligents », en étudiant notamment la communication numérique [5, 6]. D'une manière générale, les « capteurs-transmetteurs intelligents » sont cependant considérés comme des « boites noires » et leurs fonctionnalités internes ne sont souvent pas prises en compte dans les évaluations. L'évaluation de la fiabilité des « capteurs-transmetteurs intelligents » doit ainsi faire face à plusieurs difficultés :

i. la complexité des systèmes, c'est-à-dire que de nombreuses interactions peuvent exister entre les éléments matériels, mais également entre les différentes fonctions du système ;
ii. le comportement du système en présence de défauts ou de défaillances qui est souvent mal connu et difficile à appréhender, notamment en raison de la présence d'unités programmées et de logiciels ;
iii. plusieurs données sont transmises par le système et peuvent être erronées de façon dépendante (résultats de mesure, informations de diagnostic) ;
iv. peu de retour d'expérience est disponible (sur les paramètres de fiabilité et les modes de défaillance) de par la nature « nouvelle » des technologies utilisées.

De ce fait, les études qualitatives telles les analyses des modes de défaillance et de leurs criticité (AMDEC) sont difficilement exhaustives à cause des points ii et iv, et limitées dans la prise en compte des défaillances multiples face aux points i et iii. De plus, les outils d'analyses binaires (diagrammes de fiabilité, arbres de défaillance) sont souvent inappropriés en l'état, en particulier à cause des points ii et iii. Enfin, les approches par transitions entre états (chaînes de Markov, réseaux de Petri) doivent faire face à certaines difficultés dans la définition des états et des transitions requis par la modélisation, en particulier à cause des points i et ii.

2.2. Modélisation à trois niveaux « 3-Step » : défauts et défaillances - éléments matériels - fonctions

Un modèle à trois niveaux (« 3-step ») a été développé [2], tout d'abord pour faire face au point i de la Section 2.1. Celui-ci est basé sur les « goal tree–success tree » (GTST) [7] afin de représenter les aspects fonctionnels et matériels du système, et inclut les défauts et défaillances en tant que troisième composante pour permettre des analyses de fiabilité. L'aspect comportemental est ensuite décrit par des matrices de relations, aussi nommées « master logic diagrams » (MLD), qui permettent de représenter les différentes relations (inter et intra) qui existent entre les défauts ou défaillances, les éléments matériels, et les fonctions du système. Un modèle « générique » pour la modélisation de « capteurs-transmetteurs intelligents », basé sur cette approche, a ainsi pu être proposé [8].

La formalisation mathématique de ce modèle a ensuite permis de réaliser des analyses de fiabilité de « capteurs-transmetteurs intelligents » [9]. Les analyses de relations ont été proposées afin d'évaluer les effets de n'importe quel défaut ou défaillance sur n'importe quel élément matériel ou fonction du système, répondant ainsi au point ii de la Section 2.1. Prenant en compte ces effets, les probabilités de dysfonctionnement de chacune des fonctions du système, ainsi que les probabilités de modes de défaillance correspondants, ont pu être évaluées en fonction du temps, répondant alors au point iii de la Section 2.1. Des analyses d'incertitudes ont également été effectuées pour répondre aux problèmes posés par le point iv de la Section 2.1. La sous-section suivante de ce papier propose une extension de ce modèle par l'utilisation de différentes portes logiques, par similitude avec les arbres de défaillance. Pour répondre aux particularités définies dans la Section 2.1, une porte dite « continue », ou « C », est introduite afin de permettre une paramétrisation de nature continue des relations entre les éléments du système (défauts ou défaillances, éléments matériels, fonctions), par opposition aux relations binaires des portes ET et OU.

2.3. Extension de la modélisation « 3-Step » avec des portes ET, OU, et C

La Figure 1 propose un extrait d'une modélisation « 3-step » étendue, illustrée par un capteur-transmetteur de gaz par absorption infrarouge. La première partie (mais « 3ème niveau ») du modèle est une décomposition fonctionnelle du système. Au sommet se trouve la *fonction globale*, qui est accomplie par l'intermédiaire de *fonctions de bases*. Les *fonctions supports* peuvent quant à elles avoir des effets « transversaux » sur les fonctions précédentes (par exemple, sur la Figure 1, l'*auto-ajustage* permet de définir des paramètres requis pour *traiter les informations de mesure*). La seconde partie (et « 2ème niveau ») du modèle est une décomposition matérielle du système. On y trouve les principaux *sous-systèmes* utilisés qui fournissent les ressources physiques pour l'accomplissement des fonctions identifiées dans la première partie. Un sous-système peut être constitué de composants regroupés sur des critères « physiques » ou « fonctionnels », et peut ensuite être décomposé en *unités de base*. Des *éléments matériels support* peuvent également être identifiés, relatifs par exemple à l'alimentation (ces derniers ne sont pas pris en compte dans l'exemple simplifié de la Figure 1). Enfin, la troisième partie (mais « 1er niveau ») du modèle dresse un inventaire de tous les défauts et défaillances (la différence entre ces deux notions est ici définie via leurs effets sur la réalisation des fonctions du système) qui peuvent affecter le fonctionnement du système.

Le dysfonctionnement de chaque élément du système (occurrence d'un défaut ou d'une défaillance, défaillance d'un élément matériel, dysfonctionnement d'une fonction) correspond à un évènement, défini par une lettre (et éventuellement un indice) accolée à l'élément en question (sur la Figure 1 : D_i, U_i, M_i, S_i, F_i, et G). Les relations entre les éléments du système sont alors représentées par des matrices de relations qui utilisent différents types de portes. Les portes ET et OU sont communes aux arbres de défaillances. Sur la Figure 1, le sous-système *capteurs de température* est par exemple constitué de deux capteurs redondants, et la défaillance de celui-ci (évènement M_4) se produit si et seulement si les *1er* et *2nd capteurs de température* sont défaillants (évènements U_2 et U_3). Pour faire face au caractère indéterminé de certaines relations (modes de défaillance mal définis, comportements mal connus du système en présence de défauts ou de défaillances), des portes à paramètres continus, dites « portes continues » ou « porte C » ont également été introduites. Comme représenté sur la Figure 2, une porte C attribue à chacun de ses évènements de base E_i un poids p_i, avec $0 \leq p_i \leq 1$ et $i = 1, \ldots, N$. L'occurrence de l'évènement sommet (*top*) d'une porte C se produit alors si :

- n'importe quel évènement de base E_i se produit et provoque, avec une probabilité p_i, l'occurrence de l'évènement sommet (relations dites « directes ») ; ou
- tous les évènements de base E_i se produisent (relation dite « logique »).

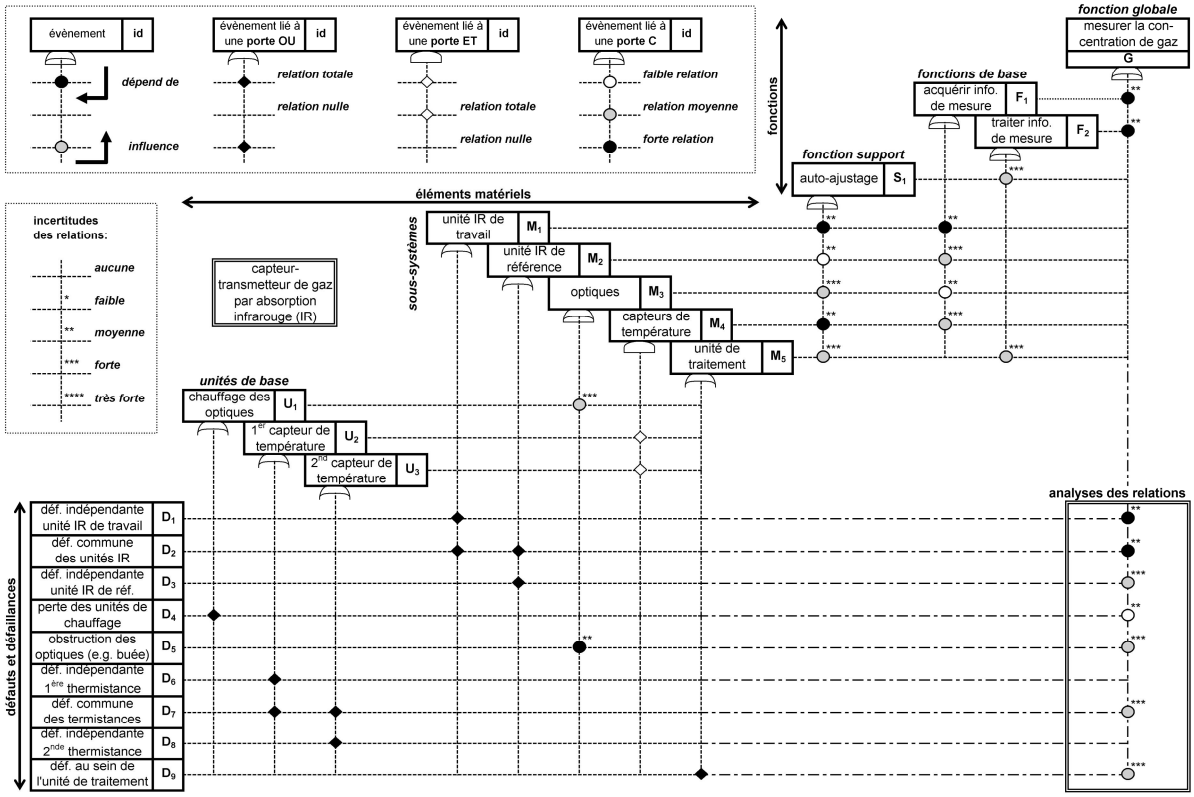

Figure 1. Extrait du modèle « 3-Step » étendu, illustré par un capteur-transmetteur de gaz par absorption infrarouge

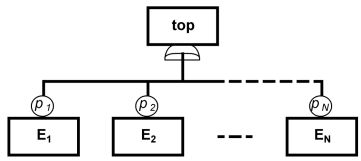

Figure 2. Porte C

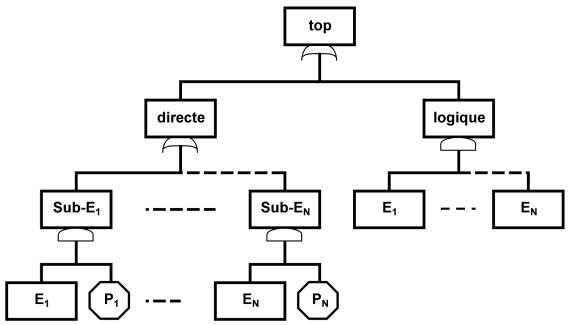

Figure 3. Arbre de défaillance équivalent à une porte C

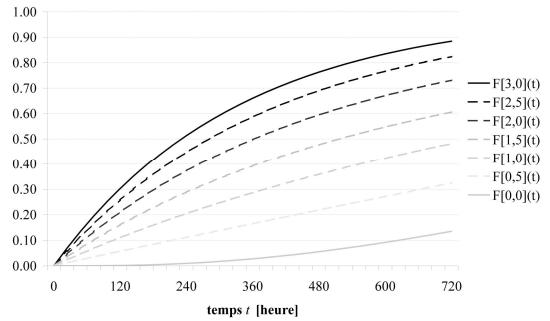

Figure 4. Résultats des fonctions de défiabilité du Tableau 1

Table 1. Exemples de fonctions de défiabilité pour une porte C

poids			fonction de défiabilité
p_1	p_2	p_3	$F_{top}(t)$
0,00	*0,00*	*0,00*	*F[0,0](t)*
0,50	*0,00*	*0,00*	*F[0,5](t)*
0,50	*0,50*	*0,00*	*F[1,0](t)*
0,50	*0,50*	*0,50*	*F[1,5](t)*
1,00	*0,50*	*0,50*	*F[2,0](t)*
1,00	*1,00*	*0,50*	*F[2,5](t)*
1,00	*1,00*	*1,00*	*F[3,0](t)*

Par l'introduction d'évènements fictifs P_i dont la probabilité d'occurrence est constante et égale à p_i, une porte C est alors équivalente à l'arbre de défaillance représenté sur la Figure 3. En notant $F_i(t)$ la probabilité que l'évènement de base E_i se produise avant l'instant t puis reste dans cet état, et $F_{top}(t)$ la probabilité d'occurrence de l'évènement sommet d'une porte C avant l'instant t (fonction de défiabilité), nous pouvons alors déduire l'expression suivante [10] :

$$F_{top}(t) = 1 - \prod_{i=1}^{N} \left(1 - p_i \cdot F_i(t)\right) + \prod_{i=1}^{N} \left((1 - p_i) \cdot F_i(t)\right) \quad \{1\}$$

La Figure 4 représente des résultats de cette fonction de défiabilité avec $N = 3$, $F_i(t) = 1\text{-}e^{-0,001 \cdot t}$ pour $i = 1,\ldots,N$, et les poids p_i donnés dans le Tableau 1. Lorsque tous les poids sont égaux à *0,00*, une porte C est alors équivalente à une porte ET (seule la relation dite « logique » peut se produire), et lorsque tous les poids sont égaux à *1,00*, une porte C est équivalente à une porte OU (selon les relations dites « directes »). De plus, la structure de tout système cohérent est comprise entre une structure parallèle (c'est-à-dire une porte ET) et série (c'est-à-dire une porte OU) [11]. En agissant sur les poids (qui sont des réels), une porte C permet alors de paramétrer de façon continue la structure d'un système entre ces deux extrêmes (cf. Figure 4).

Table 2. Taux de défaillance

nom	valeur de base	analyses d'incertitudes		
		loi*	moyenne	variance
λ_1	$4{,}00 \cdot 10^{-7}$	Log-Normale	$4{,}00 \cdot 10^{-7}$	$3{,}17 \cdot 10^{-14}$
λ_2	$1{,}00 \cdot 10^{-7}$	Log-Normale	$1{,}00 \cdot 10^{-7}$	$1{,}98 \cdot 10^{-15}$
λ_3	$4{,}00 \cdot 10^{-7}$	Log-Normale	$4{,}00 \cdot 10^{-7}$	$3{,}17 \cdot 10^{-14}$
λ_4	$1{,}00 \cdot 10^{-6}$	Log-Normale	$1{,}00 \cdot 10^{-6}$	$1{,}98 \cdot 10^{-13}$
λ_5	$3{,}00 \cdot 10^{-6}$	Log-Normale	$3{,}00 \cdot 10^{-6}$	$1{,}78 \cdot 10^{-12}$
λ_6	$5{,}00 \cdot 10^{-7}$	Log-Normale	$5{,}00 \cdot 10^{-7}$	$4{,}95 \cdot 10^{-14}$
λ_7	$1{,}50 \cdot 10^{-7}$	Log-Normale	$1{,}50 \cdot 10^{-7}$	$4{,}45 \cdot 10^{-15}$
λ_8	$5{,}00 \cdot 10^{-7}$	Log-Normale	$5{,}00 \cdot 10^{-7}$	$4{,}95 \cdot 10^{-14}$
λ_9	$5{,}00 \cdot 10^{-7}$	Log-Normale	$5{,}00 \cdot 10^{-7}$	$4{,}95 \cdot 10^{-14}$

*définies pour obtenir des facteurs d'erreur égaux à *5.00*

Table 3. Poids des portes C

type de relation	valeur de base	analyses d'incertitudes		
		loi*	moyenne	variance
faible	*0,10*	U[*0,0* ; *0,2*]	*0,10*	$3{,}33 \cdot 10^{-3}$
moyenne	*0,50*	U[*0,2* ; *0,8*]	*0,50*	$3{,}00 \cdot 10^{-2}$
forte	*0,90*	U[*0,8* ; *1,0*]	*0,90*	$3{,}33 \cdot 10^{-3}$

*U[*a* ; *b*] est une loi uniforme continue entre *a* et *b*

Table 4. Représentation graphique des effets*

effet	type de relation associée
inférieur à *0.20*	faible
entre *0.20* et *0.80*	moyenne
supérieure à *0.80*	forte

*effets des défauts et défaillances sur la fonction globale, définis par des probabilités conditionnelles (cf. Section 2.4)

Table 5. Représentation graphique des incertitudes

type d'incertitude	représentation graphique	ordre de grandeur des variances
aucune / très faible		10^{-5} et inférieur
faible	*	10^{-4}
moyenne	**	10^{-3}
forte	***	10^{-2}
très forte	****	10^{-1} et supérieur

2.4. Premières analyses à partir du modèle « 3-step » étendu

Afin d'effectuer les analyses à partir d'outils disponibles en sûreté de fonctionnement, le modèle de la Figure 1 a été traduit avec des arbres de défaillances, en utilisant des arbres de défaillances équivalents aux portes C (cf. Figure 3) et des évènements fictifs correspondant aux poids de ces portes. La probabilité d'occurrence de chaque défaut ou défaillance (évènement D_i avec $i = 1, \ldots, 9$, cf. Figure 1) avant l'instant t est définie par $F_{Di}(t) = 1\text{-}e^{-\lambda i \cdot t}$, avec les taux de défaillances λ_i donnés dans le Tableau 2 (colonne « valeur de base »). Pour les portes C, à chaque type de relation telle que représenté sur la Figure 1 (faible, moyenne, forte) est associé un poids qui est défini dans le Tableau 3 (colonne « valeur de base »). Aucune action de maintenance n'a été considérée sur toute la période d'analyse. Les résultats ont alors été obtenus grâce à SimTree, le module d'Aralia WorkShop [12] qui permet les analyses d'arbres de défaillances. La probabilité de dysfonctionnement de la fonction globale *mesurer la concentration de gaz* (évènement G) à l'instant $t = 8760$ h (i.e. $t = 1$ an) est alors évaluée à $F_G(8760\text{ h}) = 1{,}75 \cdot 10^{-2}$.

Des indicateurs cherchant à répondre aux comportements dysfonctionnels mal connus du système (cf. point ii de la Section 2.1) sont obtenus par des analyses de relations [9]. Ceux-ci permettent d'évaluer les effets de n'importe quel défaut ou défaillance sur n'importe quel élément matériel ou fonction du système. Ils sont calculés comme la probabilité d'un dysfonctionnement, conditionnelle à l'occurrence d'un défaut ou d'une défaillance spécifique et à la non-occurrence des autres défauts et défaillances. Ces indicateurs sont alors fonction des relations entre les éléments du système, mais indépendants du temps *t*. Pour l'application présentée ici, les analyses de relations portent sur les effets des défauts et défaillances sur le dysfonctionnement de la fonction globale. C'est-à-dire que l'effet du défaut ou de la défaillance *i* (avec $i = 1, \ldots, 9$) est calculé comme la probabilité de dysfonctionnement de la fonction globale *mesurer la concentration de gaz* (évènement G), sachant l'occurrence du défaut ou de la défaillance *i* (évènement D_i) et la non-occurrence des autres défauts et défaillances (évènements non-D_j avec $j \neq i$). Les résultats obtenus ont été traduits graphiquement sur la Figure 1 (« analyses des relations »), d'après le Tableau 4. À partir de ces résultats et des taux de défaillance du Tableau 2, un encadrement précis de la probabilité de dysfonctionnement de la fonction globale peut également être directement évalué [9].

2.5. Analyses d'incertitudes à partir du modèle « 3-step » étendu

Nous pouvons distinguer deux types d'incertitudes : celles liées aux modèles, c'est-à-dire relatives aux relations définies entre les éléments ; et celles liées aux paramètres, c'est-à-dire relatives aux données d'entrée des modèles [13]. Si les analyses d'incertitudes liées aux paramètres (par exemple les taux de défaillance) sont communes dans les analyses de fiabilité [14], les analyses d'incertitudes liées aux modèles sont beaucoup plus rares. En effet, la plupart des modèles utilisés en fiabilité nécessitent de définir strictement et de façon discrète les relations entre les éléments considérés, comme par exemple dans le choix d'une porte d'un arbre de défaillance ou d'une transition d'une chaîne de Markov. Il est alors difficile d'effectuer de façon cohérente des analyses d'incertitudes de modèles, comme il est courant de le faire pour les incertitudes paramétriques, car modifier de façon aléatoire les propriétés du modèle amènerait souvent à des configurations irréalistes. En exploitant des portes C, le modèle proposé possède cependant, par nature, la capacité d'effectuer des analyses d'incertitudes liées aux relations entre les éléments, qui sont définies par des paramètres continus. Ce modèle permet donc à la fois de prendre en compte des incertitudes liées aux paramètres (les taux de défaillance) et au modèle (par l'intermédiaire des poids des portes C).

Afin d'évaluer les impacts respectifs des incertitudes liées aux paramètres et au modèle, différentes configurations sont proposées telles que décrites dans le Tableau 6. Sont considérées dans une première configuration, uniquement les incertitudes paramétriques (taux de défaillance), dans une seconde configuration, uniquement les incertitudes de modèle (poids des portes C), et dans une troisième configuration, ces deux types d'incertitudes. Dans les configurations 1 et 3, les taux de défaillance sont alors modélisés par des lois Log-Normales telles que décrites dans le Tableau 2, et dans les configurations 2 et 3, les poids des portes C sont modélisés par des lois Uniformes telles que décrites dans le Tableau 3 (colonnes « analyses d'incertitude »). Pour chaque configuration, les analyses ont été effectuées sur la probabilité de dysfonctionnement de la fonction globale *mesurer la concentration de gaz* (évènement G) à l'instant $t = 8760$ h $= 1$ an, c'est-à-dire $F_G(8760\text{ h})$, en utilisant 1.000.000 simulations de Monte Carlo. Les variances alors obtenues sont reportées dans le Tableau 6, et les allures correspondantes des densités de probabilité sont représentées sur la Figure 5. Dans le cas où des incertitudes liées aux poids des portes C (incertitudes de modèle) sont considérées, les résultats d'analyses des relations sont également sujets à des incertitudes, et les variances alors obtenues ont été traduites graphiquement sur la Figure 1, d'après le Tableau 5.

Table 6. Configurations considérées pour les analyses d'incertitudes, et résultats

configu-ration	incertitude sur	F_G(8760 h = 1 an) moyenne*	variance*
1	taux de défaillance (paramètres)	$1{,}74 \cdot 10^{-2}$	$6{,}20 \cdot 10^{-5}$
2	poids des portes C (modèle)	$1{,}75 \cdot 10^{-2}$	$1{,}17 \cdot 10^{-5}$
3	taux de défaillance et poids des portes C (paramètres et modèle)	$1{,}74 \cdot 10^{-2}$	$7{,}97 \cdot 10^{-5}$
0	aucune	$1{,}75 \cdot 10^{-2}$	-

*obtenus par 1.000.000 de simulations de Monte Carlo

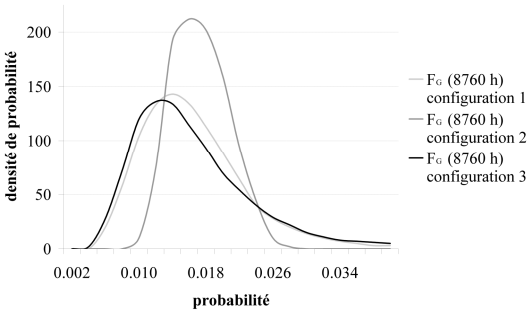

Figure 5. Densités de probabilité de F_G(8760 h), (cf. Table 6)

D'après les variances, on constate alors que les incertitudes dans les résultats (à la fois pour les analyses de relations et pour F_G(8760 h)) sont relativement faibles, notamment par rapport aux incertitudes de modèles (les ordres de grandeurs des variances des résultats sont égaux ou inférieurs à ceux des variances des poids des portes C utilisées en données d'entrée). De plus, en prenant en compte les incertitudes paramétriques, l'ajout des incertitudes de modèle n'entraîne pas d'effets très importants (par comparaison des résultats des configurations 1 et 3). On peut ainsi conclure que le modèle proposé est « robuste », c'est-à-dire que même en présence de relations incertaines entre les éléments, des évaluations de la fiabilité peuvent être menées avec des niveaux de confiance relativement bons (des démonstrations ont été apportées à cela [15]).

3. Fiabilité des « Capteurs-Transmetteurs Intelligents » en tant qu'Élément d'un Système

3.1. Les « Capteurs-transmetteurs intelligents » en tant qu'éléments d'un système de contrôle-commande

Après avoir étudié les « capteurs-transmetteurs intelligents » de façon « autonome » dans la Section 2, nous considérons ici des systèmes de contrôle-commande intégrant plusieurs de ces capteurs-transmetteurs. L'utilisation de « capteurs-transmetteurs intelligents » au sein d'un système de contrôle permet la délocalisation de certaines opérations traditionnellement effectuées par une unité centrale (cf. Section 1.3), formant ainsi un « système de contrôle distribué ». De plus, lorsque plusieurs de ces capteurs font partie d'un même « système de contrôle en réseau », ils peuvent également tirer avantage d'une communication numérique et bidirectionnelle pour s'échanger plusieurs types d'informations (résultats de mesure, informations de diagnostic) afin d'optimiser leurs opérations par l'intermédiaire de certaines fonctionnalités (comme par exemple, la correction d'erreurs de mesure, l'auto-ajustage, l'autodiagnostic, et la reconfiguration en ligne). Des critères de sûreté de fonctionnement ont été évalués pour de tels systèmes, sous l'angle de la communication numérique [5, 6] ou des capteurs [16], en utilisant des réseaux de Petri stochastiques et colorés. L'approche développée dans la suite de ce papier propose de considérer un tel système dans sa globalité, c'est-à-dire de prendre en compte les interactions entre les différents composants du système (et notamment entre les « capteurs-transmetteurs intelligents »), et du processus contrôlé. La fiabilité dynamique est alors l'outil de modélisation mathématique adapté à cette problématique [17].

3.2. Formulation du problème de fiabilité dynamique adapté aux « capteurs-transmetteurs intelligents »

Les premières méthodes de fiabilité dynamique ont émergé à la fin des années 1980 afin de prendre en compte explicitement l'influence du temps, du processus contrôlé, et des opérations humaines, sur les comportements fonctionnels et dysfonctionnels des systèmes [17]. Plus récemment, l'utilisation de systèmes à fonctionnalités numériques a également introduit de nouvelles problématiques, notamment liées à certaines interactions entre les composants du système [18]. La formulation mathématique de la fiabilité dynamique a été établie sous le nom de la théorie des « arbres d'évènements continus » (CET) [19]. Cette dernière a introduit deux types de variables utilisées pour décrire l'état d'un système : les variables (discrètes) d'état des composants, et les variables (continues) du processus contrôlé. Ces variables sont interdépendantes et évoluent à la fois de façon stochastique (par exemple la défaillance d'un composant en fonction de la température) et déterministe (par exemple un flux en fonction de l'état d'une vanne), décrivant alors un processus (markovien) déterministe par morceaux (PDP) [20].

En plus du temps t, quatre types de variables sont utilisées dans la suite de ce papier. Les variables d'état des composants sont représentées par le vecteur d'entiers noté $\boldsymbol{i(t)}$ et les variables du processus sont représentées par le vecteur de réels noté $\boldsymbol{x(t)}$, telles que définies par la théorie des CET. Afin de prendre en compte les particularités des « capteurs-transmetteurs intelligents », des variables dites « d'information » sont également introduites, représentées par un vecteur de réels noté $\boldsymbol{y(t)}$. Enfin, des variables dites « de déviation » permettent d'étendre les possibilités de modélisation des défauts et défaillances, et sont représentées par un vecteur de réels noté $\boldsymbol{e(t)}$. Ces variables sont décrites et explicitées dans les paragraphes suivants.

Les variables d'état des composants du système, notées $\boldsymbol{i(t)}$, représentent la configuration du système selon les états opérationnels et dysfonctionnels de ses composants (incluant les modes dégradés). L'état de chacun des composants est alors décrit par un entier qui constitue une composante du vecteur $\boldsymbol{i(t)}$. Les variables d'états peuvent évoluer de façon déterministe ou stochastique, en fonction des variables du processus et d'information (par exemple, l'ouverture d'une vanne est contrôlée par un signal i.e. une variable d'information ; et le taux de défaillance d'un capteur dépend de la température i.e. une variable du processus), ainsi que des variables de déviation (par exemple, après un certain niveau de dégradation i.e. une variable de déviation, un composant atteint un état dysfonctionnel complet), et parfois explicitement du temps (par exemple, des taux de défaillance sont croissants en fonction du temps). Le taux de transition des composants depuis l'état $\boldsymbol{i}^k$ vers l'état $\boldsymbol{i}^l$, étant données les variables du processus, d'information, et de déviation à l'instant t, est noté $p(\boldsymbol{i}^k \rightarrow \boldsymbol{i}^l \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t)$. Le taux de transition total des composants depuis l'état $\boldsymbol{i}^k$ est alors :

$$\lambda_{ik}(\boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t) = \sum_{i^l \neq i^k} p(\boldsymbol{i}^k \rightarrow \boldsymbol{i}^l \mid \boldsymbol{x(t)}, \boldsymbol{y(t)}, \boldsymbol{e(t)}, t) \qquad \{2\}$$

Les variables du processus ***x(t)*** représentent les variables physiques qui décrivent le processus contrôlé (e.g. pressions, températures, volumes). Elles évoluent de façon déterministe, en fonction des variables d'état des composants et de déviation (par exemple, le niveau d'un réservoir est déterminé par la configuration des vannes i.e. des variables d'état des composants, et par des niveaux de fuite i.e. des variables de déviation). Les évolutions des variables du processus peuvent alors généralement être définies par un ensemble d'équations différentielles (non-stochastiques) du premier degré :

$$\frac{d}{dt}\,\boldsymbol{x(t)} = \boldsymbol{x'(i(t), x(t), e(t), t)} \qquad \{3\}$$

Les variables d'information ***y(t)*** représentent les données et les informations qui sont traitées, stockées, et/ou échangées entre les composants du système (e.g. commandes, signaux, résultats de mesures, informations de diagnostics). Par nature, elles n'influencent pas directement les variables du processus et de déviation, mais peuvent être utilisées pour définir des changements d'états des composants. Les variables d'information peuvent généralement être exprimées directement en fonction des variables d'état des composants, du processus, et de déviation (par exemple, lorsqu'un capteur est dans un état opérationnel dégradé i.e. une variable d'état des composants, ses résultats de mesures dépendent de la quantité mesurée i.e. une variable du processus, et de dérives i.e. des variables de déviation). Ces variables peuvent également dépendre de leurs précédentes valeurs (par exemple, lorsque des données stockées sont exploitées, ou qu'un signal est bloqué sur sa valeur présente), qui sont notées $\bar{}\boldsymbol{y(t)}$ avec $\bar{}\boldsymbol{y(t)} = \boldsymbol{y(t - \varepsilon)}$ et ε un réel qui tend positivement vers la valeur nulle :

$$\boldsymbol{y(t)} = \boldsymbol{y(i(t), x(t), \bar{}y(t), e(t), t)} \qquad \{4\}$$

Les variables de déviation ***e(t)*** représentent les erreurs et les déviations de nature continue qui affectent certaines propriétés du système (e.g. dégradations de composants, dérives de paramètres). Elles évoluent de façon stochastique, en fonction des variables d'état des composants et du processus (par exemple, lorsqu'une vanne est en position fermée et dans un état dégradé i.e. une variable d'état des composants, un niveau de fuite suit une variable aléatoire influencée par la pression i.e. une variable du processus). Parce que ces évolutions sont continues, elles peuvent généralement être définies par un ensemble d'équations différentielles du premier degré, dont les dérivées sont (ou incluent) des variables aléatoires :

$$\frac{d}{dt}\,\boldsymbol{e(t)} = \boldsymbol{E'(i(t), x(t), e(t), t)} \qquad \{5\}$$

Avec ***E'(i(t), x(t), e(t), t)*** qui est un vecteur de variables aléatoires exprimant la dérivée de ***e(t)***.

3.3. Formalisme en réseau de Petri pour les analyses de fiabilité dynamique

Afin de simuler et d'analyser les évolutions du système au cours du temps, une approche numérique est choisie. Pour cela, un intervalle de temps Δt est utilisé, qui doit être assez petit pour que l'hypothèse selon laquelle les variables ***i(t)***, ***x(t)***, ***y(t)***, ***e(t)*** et t sont constantes dans tout intervalle $[t, t + \Delta t[$, soit raisonnable. Les valeurs des variables aux instants $t + \Delta t$ peuvent alors être déterminées d'après les valeurs aux instants t, en fonction des équations {2} à {5} et en utilisant des développements de Taylor et des différences finies. En particulier, les transitions des composants entre deux états qui se produisent entre les instants t et $t + \Delta t$ sont considérées comme se produisant exactement aux instants $t + \Delta t$. De même, les évolutions des variables du processus, d'information, et de déviation entre les instants t et $t + \Delta t$ sont considérées comme des « sauts » se produisant exactement aux instants $t + \Delta t$.

L'outil proposé pour effectuer ces analyses repose sur les réseaux de Petri. Ces derniers, notamment de par leurs extensions stochastiques et colorées, possèdent des caractéristiques qui en font des outils relativement naturels pour modéliser des systèmes dynamiques. En particulier, des réseaux de Petri stochastiques ont été utilisés pour des évaluations de sûreté de fonctionnement de systèmes présentant certaines de ces caractéristiques [21]. Ici, un formalisme en réseaux de Petri est présenté, exploitant des caractéristiques stochastiques et colorées, afin de :

- modéliser de façon flexible la fiabilité dynamique d'un système avec l'aide d'une interface facilement manipulable ;
- simuler les évolutions des variables du système d'après les équations {2} à {5}, selon une approche numérique ;
- effectuer des analyses de fiabilité par des simulations de Monte Carlo.

Dans l'approche développée, chaque place du réseau de Petri est associée à un jeu de variables, et vice-versa. Ainsi, le nombre de places est linéairement dépendant du nombre de variables, ce qui évite les problèmes d'explosion combinatoire lors de la modélisation. Les valeurs des variables sont directement données par les jetons (« colorés »), qui sont ici des nombres réels ou entiers, à l'intérieur des places, et sont modifiés par les transitions. En permanence, chaque place contient donc un et un seul jeton, et toutes les transitions sont exécutables. Des gardes sont alors utilisées pour chaque transition et notées $s_j[\Delta t]$, ce qui signifie que la transition est exécutée aux instants $s_j + k \cdot \Delta t$, avec $k = 0, 1, 2, \ldots$

Chaque transition du réseau de Petri est associée à une place particulière qui est la « place manipulée ». Cette dernière est reliée à la transition par un arc d'entrée, ce qui signifie que les variables représentées par cette place sont modifiées par la transition (« le jeton est retiré de la place ») ; et reliée à la même transition par un arc de sortie qui attribue aux variables leurs nouvelles valeurs (« un nouveau jeton est déposé dans la place »), selon l'expression spécifiée sur cet arc. Ces nouvelles valeurs peuvent être fonction des valeurs précédentes de cette même variable (manipulées par l'arc d'entrée), de variables aléatoires, ainsi que de variables représentées par d'autres places. Ces dernières places sont alors des « places de dépendance » et sont reliées à la transition par des arcs bidirectionnels, ce qui signifie que les variables peuvent être utilisées par la transition, mais sans les modifier.

Un réseau de Petri générique pour les analyses de fiabilité dynamique est représenté sur la Figure 6. Les cinq types de variables définies dans la Section 3.2 y sont représentés. Selon la nature des variables (continue ou discrète, stochastique ou déterministe), différentes représentations graphiques sont utilisées. Les variables sont ici données sous forme de vecteurs (excepté pour le temps t qui est un scalaire). Pour une modélisation plus détaillée, il est cependant souhaitable de diviser chaque vecteur en sous-ensembles de composants, et de traiter ces derniers séparément par des places distinctives. Chaque transition est alors exécutée à chaque intervalle de temps Δt, modifiant les variables représentées par la « place manipulée », selon les équations {2} à {5} et en utilisant des développements de Taylor et des différences finies, telles que spécifiées sur les arcs de sortie des transitions. Pour le cas le plus simple, la transition qui modifie la variable du temps t ne possède pas de « place de dépendance » et est simplement utilisée pour incrémenter la valeur du temps t par Δt à chaque exécution.

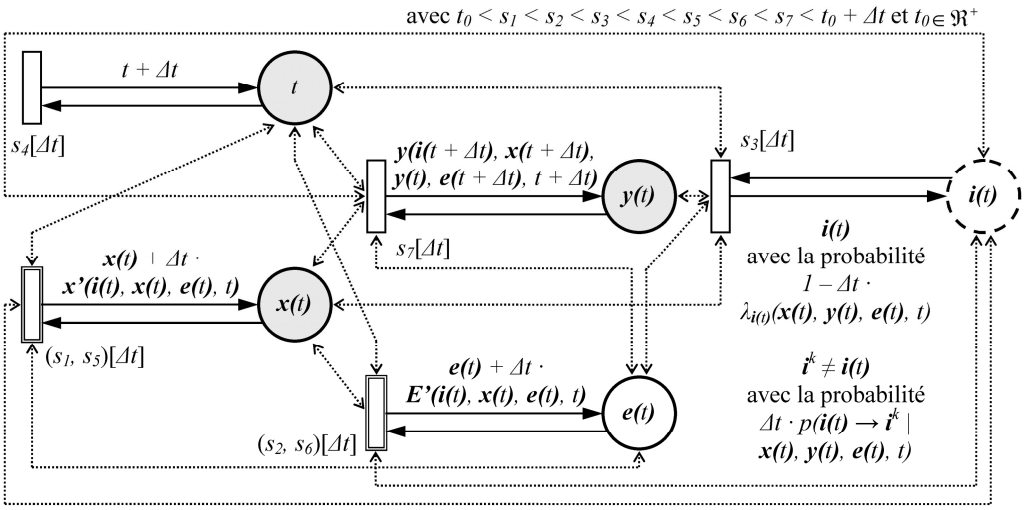

Figure 6. Réseau de Petri générique pour les analyses de fiabilité dynamique

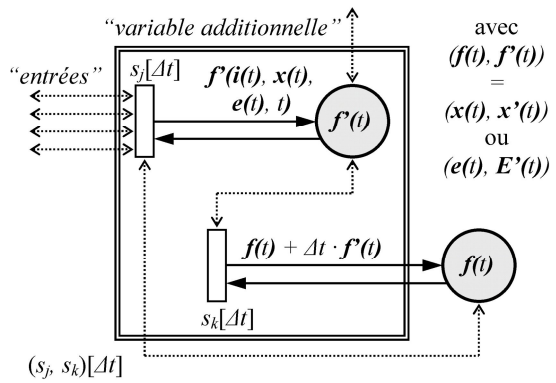

Figure 7. Méta-transition pour les réseaux de Petri

$s_j[\Delta t]$ signifie que la transition correspondante est exécutée aux instants $s_j + k \cdot \Delta t$, avec $k = 0, 1, 2, \ldots$ Dans chaque intervalle $[t, t + \Delta t]$, toutes les valeurs des variables à l'instant $t + \Delta t$ sont donc calculées suivant l'ordre qui est défini par les s_j (spécifié en haut de la Figure 6). À noter que les variables à l'instant $t + \Delta t$ dépendent des variables à l'instant t. En particulier, $\boldsymbol{x(t + \Delta t)}$ et $\boldsymbol{e(t + \Delta t)}$ dépendent tous deux à la fois de $\boldsymbol{x(t)}$ et $\boldsymbol{e(t)}$. Ainsi, pour éviter de « perdre » la valeur $\boldsymbol{x(t)}$ (resp. $\boldsymbol{e(t)}$) après le calcul de $\boldsymbol{x(t + \Delta t)}$ (resp. $\boldsymbol{x(t)}$), des « méta-transitions » sont introduites telles que décrites sur la Figure 7. Celles-ci sont utilisées pour calculer dans un premier temps toutes les dérivées à l'instant t ($\boldsymbol{x'(i(t), x(t), e(t), t)}$ et $\boldsymbol{E'(i(t), x(t), e(t), t)}$), stocker ces dernières en tant que variables additionnelles, puis enfin modifier les variables du système. Les « méta-transitions » ont donc des doubles gardes, notées $(s_j, s_k)[\Delta t]$, qui signifient que les dérivées sont calculées à chaque instant $s_j + k \cdot \Delta t$, et les variables des « place manipulées » à chaque instant $s_k + k \cdot \Delta t$ (cf. Figure 6 et 7).

3.4. Cas d'étude d'un système de sécurité intégrant des « capteurs-transmetteurs intelligents »

Le cas d'étude présenté ici est un modèle simplifié de circuit primaire du réacteur rapide Europa. Par rapport au modèle original issu de la littérature [22], les variables du processus ont été simplifiés, de nouvelles fonctionnalités ont été intégrées aux capteurs-transmetteurs (communication numérique bidirectionnelle, traitement interne des données, correction des dérives), et des variables de déviation ont été ajoutées.

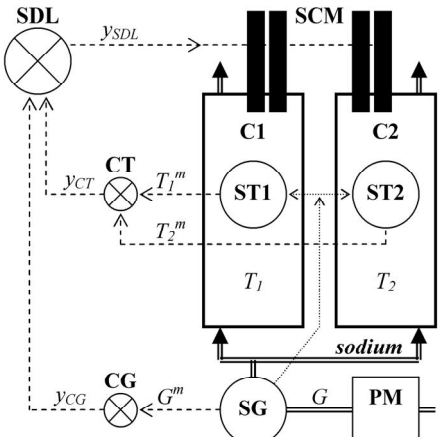

Figure 8. Réacteur Europa

Table 7. Variables d'états des composants

composant du système	variable d'état	valeur et description
pompe (PM)	*SPM(t)*	*= 1* : opération normale *= 0* : défaillance totale i.e. couple de la pompe nul *= 3* : mode dégradé i.e. couple sujet à déviation
capteur-trans. de flux (SG)	*SSG(t)*	*= 1* : résultats exacts i.e. $G^m(t)=G(t)$ *= 0* : bloqué à la valeur courante i.e. $G^m(t)=G^m(t-\varepsilon)$ *= 2* : bloqué en sécurité i.e. $G^m(t) \leq G_{min}$
contrôleur de flux (CG)	*SCG(t)*	*= 1* : signal correct i.e. $y_{CG}(t)=1$ ssi $G^m(t) \leq G_{min}$ *= 0* : bloqué à la valeur courante i.e. $y_{CG}(t)=y_{CG}(t-\varepsilon)$ *= 2* : bloqué en « sécurité » i.e. $y_{CG}(t)=1$
capteur-trans. de température (STi) *i = 1, 2*	*SSTi(t)*	*= 1* : résultats exacts i.e. $T_i^m(t)=T_i(t)$ *= 0* : bloqué à la valeur courante i.e. $T_i^m(t)=T_i^m(t-\varepsilon)$ *= 2* : bloqué en sécurité i.e. $T_i^m(t) \geq T_{max}$ *= 3* : sujet à des dérives négatives i.e. $T_i^m(t)<T_i(t)$ *= 4* : sujet à des dérives positives i.e. $T_i^m(t)>T_i(t)$
contrôleur de température (CT)	*SCT(t)*	*= 1* : signal correct i.e. $y_{CT}(t)=1$ ssi $T_i^m(t) \geq T_{max}$ $i=1$ou2 *= 0* : bloqué à la valeur courante i.e. $y_{CT}(t)=y_{CT}(t-\varepsilon)$ *= 2* : bloqué en « sécurité » i.e. $y_{CT}(t)=1$
contrôleur central (SDL)	*SSDL(t)*	*= 1* : signal correct i.e. $y_{SDL}(t)=1$ ssi $y_{CG}(t)+y_{CT}(t) \geq 1$ *= 0* : bloqué à la valeur courante i.e. $y_{SDL}(t)=y_{SDL}(t-\varepsilon)$ *= 2* : bloqué en « sécurité » i.e. $y_{SDL}(t)=1$
SCRAM (SCM)	*SSCM(t)*	*= 1* : opération normale i.e. peut être activé *= 0* : défaillance totale i.e. ne peut pas être activé *= 5* : opération de sécurité i.e. le SCRAM est activé

Table 8. Exemples de scénarios

scenario*	*SPM(t)* =	*SSCM(t)* =
a	*1* pour $t < 30$ s *0* pour $t \geq 30$ s	*1* pour $t < 35$ s *5* pour $t \geq 35$ s
b	*3* pour tout *t*	*1* pour $t < 58$ s *5* pour $t \geq 58$ s
c	*3* pour tout *t*	*0* pour tout *t*

*Lorsque que la pompe est en mode dégradé (*SPM(t) = 3*), la déviation du couple de la pompe est simulée selon un processus stochastique (cf. Équation {5}), différents résultats sont alors obtenus pour les scénarios b et c

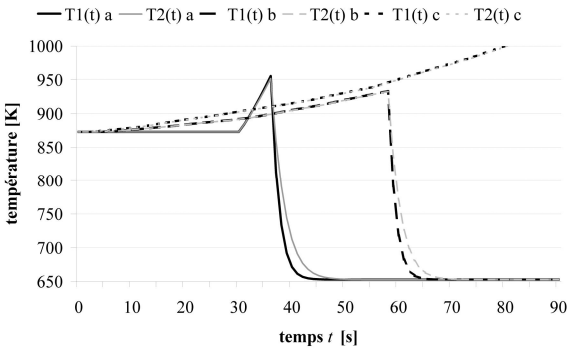

Figure 9. Exemples d'évolutions des températures de sodium selon les scénarios du Tableau 8

Le modèle simplifié du réacteur Europa est représenté sur la Figure 8. Ce système comprend deux canaux (C1 et C2), dont le circuit de refroidissement utilise du sodium introduit par une pompe (PM). Le manque de sodium, par exemple en cas de défaillance de la pompe, entraîne une augmentation de la température dans les canaux et peut provoquer des évènements accidentels. La température du sodium dans chaque canal (T_1 et T_2) est donc mesurée par des capteurs-transmetteurs de température (ST1 et ST2) qui transmettent leurs résultats de mesure (T_1^m et T_2^m) à un contrôleur commun (CT). De même, le flux de sodium (G) est mesuré par un capteur-transmetteur de flux (SG) qui transmet ses résultats de mesure (G^m) à un autre contrôleur (CG). CT et CG transmettent des signaux binaires (y_{CT} et y_{CG}) à un contrôleur central (SDL). Si un seuil haut de température (T_{max}), ou un seuil bas de flux (G_{min}) est détecté, SDL doit alors transmettre un signal binaire (y_{SDL}) qui active un système d'arrêt d'urgence (SCM). Ce dernier, communément appelé SCRAM, a pour objet d'introduire dans le cœur du réacteur des barres de sécurité qui stoppent la réaction en absorbant une forte quantité de neutrons.

L'état de chaque composant du système est représenté par un entier tel que décrit dans le Tableau 7. L'état des composants mécaniques (la pompe et le SCRAM) affecte directement les variables du processus, l'état des capteurs-transmetteurs et des contrôleurs affecte les variables d'information, tandis que les effets des modes dégradés (pour la pompe) et des dérives (pour les capteurs-transmetteurs de température) sont modélisés par des variables de déviation. Les expressions des taux transition entre les états des composants, ainsi que les équations différentielles qui définissent les évolutions des variables du processus, ne sont pas précisées ici mais peuvent être trouvées dans la littérature [23]. Notons cependant que certains taux de transition dépendent du temps t (par exemple selon une loi de Weibull), des variables d'états d'autres composants (selon des modes communs de défaillance), du processus (par exemple, les températures influencent des taux de défaillance), et de déviation (la déviation du couple de la pompe influence le taux de défaillance de cette dernière). Concernant les variables du processus, les évolutions des températures $T_1(t)$ et $T_2(t)$, en fonction des variables d'état des composants mécaniques (*SPM(t)* et *SSCM(t)*, cf. Tableau 7) sont représentées sur la Figures 9, d'après les scénarios décrits dans le Tableau 8.

Les résultats de mesure des capteurs-transmetteurs ($G^m(t)$, $T_1^m(t)$, et $T_2^m(t)$) et les signaux des contrôleurs ($y_{CG}(t)$, $y_{CT}(t)$, et $y_{SDL}(t)$) sont des variables d'information qui dépendent des variables d'état des composants, du processus, et sont également interdépendantes, tel que décrit dans le Tableau 7. Lorsque les capteurs-transmetteurs de température sont dans des états dégradés, leurs résultats de mesure sont sujets à des dérives. Ces dernières sont modélisées par des variables de déviation qui sont ajoutées ou soustraites (suivant le sens des dérives) aux résultats de mesure. Les évolutions de ces dérives suivent des processus stochastiques continus, en accord avec l'équation {5}, qui dépendent des températures (variables du processus), et dont des expressions peuvent être trouvées dans la littérature [23]. Afin de compenser ces dérives, les capteurs-transmetteurs de températures sont capables d'évaluer, par un traitement interne des données, des paramètres qui sont fonction des résultats de mesure de l'ensemble des capteurs-transmetteurs, obtenus grâce à la communication numérique bidirectionnelle. Ces paramètres dépendent des valeurs courantes ($G^m(t)$, $T_1^m(t)$, et $T_2^m(t)$) et précédentes ($G^m(t-\varepsilon)$, $T_1^m(t-\varepsilon)$, et $T_2^m(t-\varepsilon)$) des résultats de mesure, et exploitent les relations théoriques qui existent entre l'évolution du flux et celles des températures ($G(t)$, $T_1(t)$, $T_2(t)$, $G(t-\varepsilon)$, $T_1(t-\varepsilon)$, et $T_2(t-\varepsilon)$). À partir de ces paramètres, les capteurs-transmetteurs peuvent ainsi déduire des caractéristiques supposées des résultats de mesure (sur ou sous-estimations des valeurs mesurées). Afin de corriger les dérives ainsi détectées, des paramètres de correction sont alors évalués et ajoutés aux résultats de mesure des capteurs-transmetteurs de températures. Les définitions précises de ces paramètres sont présentes dans la littérature [23].

3.5. Analyses de fiabilité dynamiques

Le cas d'étude présenté dans la Section 3.4 a été modélisé en suivant le formalisme en réseaux de Petri présenté dans la Section 3.3. Un total de 53 places et 53 transitions a été nécessaire pour représenter entièrement le cas d'étude, ce qui est relativement peu compte tenu du nombre très important d'interactions qui existent au sein de ce système et donc du nombre considérable d'états possibles pour le système dans son ensemble.

Les simulations et les analyses ont été effectuées à l'aide du logiciel CPN Tools [24]. Différents scénarios ont été définis à partir d'un évènement initiateur qui est une défaillance (mode dégradé ou défaillance totale) de la pompe de sodium, ce qui implique une augmentation des températures et doit conduire à l'activation du SCRAM une fois certains seuils atteints (cf. Tableau 8 et Figure 9 pour un seuil de température proche de *930* K). Ces scénarios ont été classés selon que l'activation du SCRAM avait lieu hors des conditions souhaitées (déclenchement intempestif), à temps (situation contrôlée), trop tard ou jamais (évènement accidentel). Les résultats obtenus par simulations de Monte Carlo ont alors permis d'étudier l'effet des fonctionnalités numériques des capteurs-transmetteurs sur la disponibilité et la sécurité du système. Ainsi, il a été montré que les corrections des dérives permettaient une forte réduction des déclenchements intempestifs, sans toutefois annuler complètement les effets des dérives (les procédures de correction des dérives peuvent être sujettes à des erreurs de diagnostics). En contrepartie, la réduction des déclenchements intempestifs implique une (légère) augmentation des évènements accidentels car augmente automatiquement le temps de « vie utile » du système, et donc les possibilités qu'une défaillance « dangereuse » puisse se produire (ces défaillances n'ayant plus lieu d'être après un déclenchement intempestif).

4. Conclusion

Pour la sûreté de fonctionnement, et plus généralement pour la maîtrise des risques technologiques, une des principales caractéristiques des « capteurs-transmetteurs intelligents » est de pouvoir mettre en balance, de par leurs fonctionnalités numériques, la disponibilité et la sécurité des systèmes. En effet, grâce aux fonctions avancées d'autodiagnostic des défauts et des défaillances, les « capteurs-transmetteurs » peuvent soit procéder à des positions de repli (activation des fonctions de sécurité), soit effectuer des procédures de compensation (corrections des erreurs de mesures, reconfigurations), la communication numérique bidirectionnelle pouvant contribuer à plusieurs de ces fonctions grâce à des « coopérations » entre capteurs. La première option privilégie la sécurité (sous condition cependant que les déclenchements intempestifs soient effectivement « sûrs »), tandis que la seconde privilégie la disponibilité des systèmes en prenant le risque que les procédures de compensation soient sujettes à des erreurs entraînant des « états dangereux non-diagnostiqués ». Afin d'effectuer les choix adéquats de management des risques sous les fortes contraintes sociétales, environnementales, et économiques, il est ainsi nécessaire de disposer d'outils adaptés à l'évaluation exhaustive de la sûreté de fonctionnement de tels systèmes.

Les travaux réalisés au cours de la thèse présentée dans la Section 1.4, et dont ce présent papier fait brièvement état, ont ainsi permis de fournir des outils efficaces et techniquement exploitables en milieu industriel pour : évaluer les performances de « capteurs-transmetteurs intelligents » et ce, même en présence de comportements dysfonctionnels incertains, et en intégrant les nombreuses interactions matérielles et fonctionnelles ; et évaluer un système de contrôle relatif à la sécurité, intégrant plusieurs « capteurs-transmetteurs intelligents », en prenant en compte les interactions entre les composants du système ainsi qu'avec le processus contrôlé, sur des bases scientifiques de la fiabilité dynamique.

Remerciements

La Section 3 de ce papier a été réalisée à l'Université d'État de l'Ohio (OSU), dans le cadre d'une collaboration scientifique entre l'INERIS, l'UTT, et OSU. Nous souhaitons ainsi remercier Pr. Carol Smidts qui a co-encadré une partie de ces travaux.

Références

[1] Ministère de l'Écologie, du Développement et de l'Aménagement Durable, 2007, « Le plan de prévention des risques technologiques (PPRT) – Guide méthodologique ».
[2] F. Brissaud, D. Charpentier, A. Barros, C. Bérenguer, 2008, « Capteurs intelligents : Nouvelles technologies et nouvelles problématiques pour la sûreté de fonctionnement », dans les actes du 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement (λμ16).
[3] F. Brissaud, A. Barros, C. Bérenguer, 2010, « Probability of Failure of Safety-Critical Systems Subject to Partial Tests », dans les actes du 56th Annual Reliability and Maintenability Symposium.
[4] F. Brissaud, D. Charpentier, M. Fouladirad, A. Barros, C. Bérenguer, 2010, « Failure rate evaluation with influencing factors », Journal of Loss Prevention in the Process Industries, vol. 23(2), p. 187-193.
[5] P. Barger, J.M. Thiriet, M. Robert, 2002, « Dynamic reliability and availability evaluation and validation of distributed systems », dans les actes de la 19th IEEE IMTC, vol. 1-2, p. 837-842.
[6] R. Ghostine, J.M. Thiriet, J.F. Aubry, 2006, « Dependability evaluation of networked control systems under transmission faults », dans les actes du 6th IFAC symposium SAFEPROCESS, vol. 6.
[7] M. Modarres, S.W. Cheon, 1999, « Function-centered modeling of engineering systems using the goal tree-success tree technique and functional primitives », Reliability Engineering and System Safety, vol. 64(2), p. 181-200.
[8] F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier, 2009, « Dependability Issues for Intelligent Transmitters and Reliability Pattern Proposal », dans les actes du 13th IFAC Symposium INCOM, vol. 13, Part 1.
[9] F. Brissaud, D. Charpentier, A. Barros, C. Bérenguer, (à paraître en 2010), « Capteurs intelligents : Nouvelles technologies et nouvelles problématiques pour la sûreté de fonctionnement », chapitre d'ouvrage dans « Anticipation, innovation, perception : des défis pour la maîtrise des risques à l'horizon 2020 » (édition à préciser).
[10] F. Brissaud, A. Barros, C. Bérenguer, D. Charpentier, 2009, « Design of complex safety-related systems in accordance with IEC 61508 », dans les actes de ESREL, p. 1555-1562.
[11] M. Rausand, A. Høyland, 2002, « System reliability theory; models, statistical methods, and applications », 2ème édition, Wiley.
[12] Aralia WorkShop, 2009, http://www.arboost.com/arlshop-page.htm
[13] US Nuclear Regulatory Commission, 2002, « An approach for using probabilities risk assessement in risk-informed decisions on plant-specific changes to the licensing basis », Regulatory guide 1.174, Revision 1, US NRC
[14] R.L. Winkler, 1996, « Uncertainty in probabilistic risk assessment », Reliability Engineering and System Safety, vol. 54, p. 127-132.
[15] F. Brissaud, A. Barros, C. Bérenguer, (à paraître), « Handling Parameter and Model Uncertainties by Continuous Gates in Fault Tree Analyses », Journal of Risk and Reliability.
[16] F. Brissaud, A. Barros, C. Bérenguer, 2010, « Improving availability and safety of control systems by cooperation between intelligent transmitters », dans les actes du 10th PSAM.
[17] P.E. Labeau, C. Smidts, S. Swaminathan, 2000, « Dynamic reliability: towards an integrated platform for probabilistic risk assessmen », Reliability Engineering and System Safety, vol. 68, p. 219-254.
[18] T. Aldemir, *et al.*, 2006, « Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments », NUREG/CR-6901, US NRC
[19] J. Devooght, C. Smidts, 1992, « Probabilistic Reactor Dynamics–I: The Theory of Continuous Event Trees », Nuclear Science and Engineering, vol. 111, p. 229-250.
[20] M.H.A. Davis, 1993, « Markov models and optimization », Chapman and Hall.
[21] Y. Dutuit, E. Chatelet, J.P. Signoret, P. Thomas, 1997, « Dependability modelling and evaluation by using stochastic Petri nets: Application to two test cases », Reliability Engineering and System Safety, vol. 55, p. 117-124.
[22] C. Smidts, J. Devooght, 1992, « Probabilistic Reactor Dynamics–II: A Monte Carlo Study of a Fast Reactor Transient », Nuclear Science and Engineering, vol. 111, p. 241-256.
[23] F. Brissaud, C. Smidts, A. Barros, C. Bérenguer, 2010, « Dynamic Reliability Modeling of Cooperating Digital-Based Systems », dans les actes de ESREL
[24] CPN Tools, http://wiki.daimi.au.dk/cpntools/cpntools.wiki